PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-215027
(43)Date of publication of application : 31.07.2002

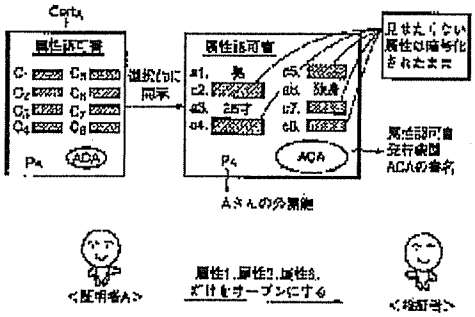
(51)Int.Cl. G09C 1/00
H04L 9/32

(21)Application number : 2001-013529
(22)Date of filing : 22.01.2001

(71)Applicant : TOSHIBA CORP
(72)Inventor : MIYAZAKI SHINGO
KAWAMURA SHINICHI

(54) ATTRIBUTE CERTIFICATION PROGRAM AND DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To realize certification and signature techniques which can be applied to various systems and contribute to development of an information-oriented society.
SOLUTION: The attribute certificate is provided which includes a lot of attribute information so that they can be individually verified. Concretely, (1) an attribute certificate CertA is a digital signature of an attribute certificate issue agency ACA which is given to a public key PA of a prover A, attribute information c1 to c8 ciphered by a key, and the total number 8 of attributes. (2) The prover A discloses attribute information a1, a3, and a6, which are related to only attributes of which the disclosure is requested, to a verifier and proves it to the verifier that disclosed attribute information a1, a3, and a6 are permitted right information. (3) Attribute information a2, a4, a5, a7, and a8 related to attributes of which the disclosure is not requested are not disclosed to the verifier at all. Thus various certificates/signatures using minimum required attributes are possible.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－215027
（P2002－215027A）
(43)公開日　平成14年７月31日(2002.7.31)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*(参考)
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ	５Ｊ１０４
			６４０Ｚ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ	
			６７５Ｄ	

審査請求　未請求　請求項の数14　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－13529(P2001－13529)

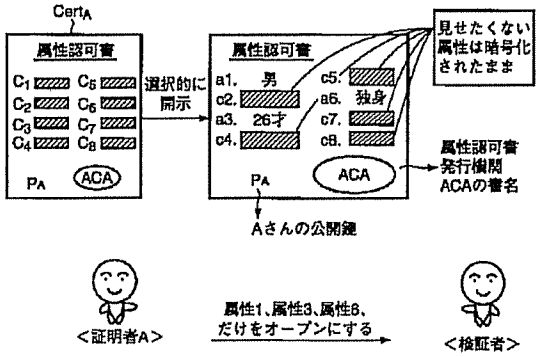
(22)出願日　平成13年１月22日(2001.1.22)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　宮崎　真悟
東京都府中市東芝町１番地　株式会社東芝府中事業所内
(72)発明者　川村　信一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5J104 AA07 KA01 KA05 LA05 MA02
NA02 NA12

(54)【発明の名称】　属性証明プログラム及び装置

(57)【要約】
【課題】　各種システムに応用でき、情報化社会の発展に寄与できる認証・署名技術を実現する。
【解決手段】　複数の属性情報を個別に検証可能に含めた属性認可書を設ける。具体的には（１）属性認可書$Cert_A$は、証明者の公開鍵P_A、鍵暗号化された属性情報c_1～c_8、及び属性の総数８、に対して施された属性認可書発行機関ＡＣＡのディジタル署名とする。（２）証明者Ａは、開示要求された属性のみに関する属性情報a_1,a_3,a_6を検証者に開示でき、また、開示された属性情報a_1,a_3,a_6が認可された正当な情報である旨を検証者に証明できる。（３）開示要求されていない属性に関する属性情報a_2,a_4,a_5,a_7,a_8は検証者に一切露呈しない。よって必要最小限の属性を用いた各種証明／署名が可能である。



1

【特許請求の範囲】

【請求項１】　ｎ個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内のｎ個の属性情報のうち、ｎ個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される属性証明プログラムであって、

前記利用者装置のコンピュータを、

前記属性認可書の発行の際に、

秘密鍵及び公開鍵を生成する鍵生成手段、

入力された内容に基づいて前記ｎ個の属性情報を生成し、当該ｎ個の属性情報及び前記鍵生成手段により生成された公開鍵を前記属性認可書発行機関装置に提示する属性情報生成手段、

前記属性認可書発行機関装置から受けた属性認可書を検証する属性認可書検証手段、として機能させ、

前記検証者装置による検証の際に、

前記属性認可書の検証用データと、チャレンジに基づいて計算した属性証明並びに前記ｎ個以下の属性情報の検証用データとを同時に又は別々に前記検証者装置に送信する属性証明生成手段、

として機能させるための属性証明プログラム。

【請求項２】　請求項１に記載の属性証明プログラムにおいて、

前記属性証明生成手段は、前記チャレンジのハッシュ値を算出し、このハッシュ値に基づいて前記属性証明を算出することを特徴とする属性証明プログラム。

【請求項３】　請求項１又は請求項２に記載の属性証明プログラムにおいて、

前記属性証明生成手段は、

「前記同時に又は別々に」に代えて「同時に」とし、且つ前記チャレンジを生成する処理を含むことを特徴とする属性証明プログラム。

【請求項４】　ｎ個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内のｎ個の属性情報のうち、ｎ個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される属性証明プログラムであって、

前記属性認可書発行機関装置のコンピュータを、

前記利用者装置から提示された各属性情報に関して正当か否かを審査する属性情報審査手段、

前記属性情報審査手段による審査結果が正当である旨を示すとき、前記ｎ個の属性情報を埋め込んで属性認可書を発行し、当該属性認可書を利用者装置に送信する属性認可書発行手段、

として機能させるための属性証明プログラム。

【請求項５】　ｎ個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内のｎ個の属性情報のうち、ｎ個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される属性証明プログラムであって、

前記検証者装置のコンピュータを、

前記利用者装置から受けた前記属性認可書の検証用データに基づいて、前記属性認可書の正当性を検証する属性認可書検証手段、

前記属性認可書検証手段による検証結果が正当性を示すとき、前記利用者装置から受けた属性証明及び前記ｎ個以下の属性情報に関し、各々正当性を検証する属性証明検証手段、

として機能させるための属性証明プログラム。

【請求項６】　請求項５に記載の属性証明プログラムにおいて、

前記検証者装置のコンピュータを、

前記属性認可書検証手段による検証結果が正当性を示すとき、ｎ個以下の属性を指定する属性情報生成手段、

前記属性情報生成手段により属性が指定されると、チャレンジを生成し、当該チャレンジ及び前記指定内容を前記利用者装置に送信するチャレンジ生成手段、

として機能させるための属性証明プログラム。

【請求項７】　請求項５又は請求項６に記載の属性証明プログラムにおいて、

前記属性証明検証手段による検証結果が正当性を示すとき、前記開示されたｎ個以下の属性情報の内容に基づいて、所定の対象システムの実行を許可する対象実行許可手段、

として機能させるための属性証明プログラム。

【請求項８】　ｎ個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内のｎ個の属性情報のうち、ｎ個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される前記利用者装置であって、

前記属性認可書の発行の際に、秘密鍵及び公開鍵を生成する鍵生成手段と、

入力された内容に基づいて前記ｎ個の属性情報を生成し、当該ｎ個の属性情報及び前記鍵生成手段により生成された公開鍵を前記属性認可書発行機関装置に提示する属性情報生成手段と、

前記属性認可書発行機関装置から受けた属性認可書を検証する属性認可書検証手段と、

前記検証者装置による検証の際に、前記属性認可書の検証用データと、チャレンジに基づいて計算した属性証明並びに前記ｎ個以下の属性情報の検証用データとを同時に又は別々に前記検証者装置に送信する属性証明生成手

段と、
を備えたことを特徴とする利用者装置。
【請求項９】　請求項８に記載の利用者装置において、
前記属性証明生成手段は、前記チャレンジのハッシュ値を算出し、このハッシュ値に基づいて前記属性証明を算出することを特徴とする利用者装置。
【請求項１０】　請求項８又は請求項９に記載の利用者装置において、
前記属性証明生成手段は、
「前記同時に又は別々に」に代えて「同時に」とし、且つ前記チャレンジを生成する処理を含むことを特徴とする利用者装置。
【請求項１１】　ｎ個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内のｎ個の属性情報のうち、ｎ個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される前記属性認可書発行機関装置であって、
前記利用者装置から提示された各属性情報に関して正当か否かを審査する属性情報審査手段と、
前記属性情報審査手段による審査結果が正当である旨を示すとき、前記ｎ個の属性情報を埋め込んで属性認可書を発行し、当該属性認可書を利用者装置に送信する属性認可書発行手段と、
を備えたことを特徴とする属性認可書発行機関装置。
【請求項１２】　ｎ個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内のｎ個の属性情報のうち、ｎ個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される前記検証者装置であって、
前記利用者装置から受けた前記属性認可書の検証用データに基づいて、前記属性認可書の正当性を検証する属性認可書検証手段と、
前記属性認可書検証手段による検証結果が正当性を示すとき、前記利用者装置から受けた属性証明及び前記ｎ個以下の属性情報に関し、各々正当性を検証する属性証明検証手段と、
を備えたことを特徴とする検証者装置。
【請求項１３】　請求項１２に記載の検証者装置において、
前記属性認可書検証手段による検証結果が正当性を示すとき、ｎ個以下の属性を指定する属性情報生成手段と、
前記属性情報生成手段により属性が指定されると、チャレンジを生成し、当該チャレンジ及び前記指定内容を前記利用者装置に送信するチャレンジ生成手段と、
を備えたことを特徴とする検証者装置。
【請求項１４】　請求項１２又は請求項１３に記載の検証者装置において、
前記属性証明検証手段による検証結果が正当性を示すとき、前記開示されたｎ個以下の属性情報の内容に基づいて、所定の対象システムの実行を許可する対象実行許可手段を備えたことを特徴とする検証者装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、各種システムに応用可能な属性証明プログラム及び装置に関する。
【０００２】
【従来の技術】近年の情報化社会では、各端末装置間でのデータ通信の際に、データの正当性を認証するディジタル署名及びメッセージ認証や、通信相手の正当性を認証する相手認証といった認証・署名技術が広く用いられている。
【０００３】係る認証・署名技術は、例えば証明者（署名者）が自己の秘密鍵情報により認証や署名を行なう方式となっている。また、検証者は、証明者（署名者）の公開鍵情報により、例えば証明者の署名を検証すればよい。
【０００４】
【発明が解決しようとする課題】以上のような認証・署名技術は、情報化社会を支える暗号技術の中でも必要性の高いものであり、情報化社会を発展させる観点から、各種の応用手法が開発されることが好ましい。
【０００５】本発明は上記実情を考慮してなされたもので、各種システムに応用でき、情報化社会の発展に寄与し得る属性証明プログラム及び装置を提供することを目的とする。
【０００６】
【課題を解決するための手段】本発明の骨子は、複数の属性情報を個別に検証可能に含めた属性認可書を設ける構成により、各種システムに応用し得る認証・署名技術を提供することにある。
【０００７】係る本発明は以下の（１）～（３）に示す性質を有する。
【０００８】（１）属性認可書$Cert_A$は、図６の例で述べると、証明者の公開鍵P_A、鍵暗号化された属性情報c_1～c_8、及び属性の総数ｎ（＝８）、に対して施された属性認可書発行機関ＡＣＡのディジタル署名である。
【０００９】（２）証明者Ａは、開示要求された属性のみに関する属性情報a_1, a_3, a_6を検証者に開示でき、また、開示された属性情報a_1, a_3, a_6が認可された正当な情報である旨を検証者に証明することができる。
【００１０】（３）開示要求されていない属性に関する属性情報a_2, a_4, a_5, a_7, a_8は検証者に一切露呈しない。よって必要最小限の属性を用いた各種証明／署名が可能である。
【００１１】係る本発明は、図７（ａ）に示す従来の秘密鍵による署名に比べ、図７（ｂ）に示すように各属性

１～３を含む署名である点で異なり、さらに、図６に示したように、各属性を選択的に開示できる点で優れている。

【００１２】さて、以上のような本発明の骨子について具体的には以下のような手段が講じられる。なお、各発明は、記載の簡潔性の観点から、プログラムとして表現された場合のみを示すが、装置、方法、システム等の他のカテゴリーで表現してもよいことは言うまでもない。

各発明の適用対象は、ｎ個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内のｎ個の属性情報のうち、ｎ個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される属性証明プログラムである。

【００１３】第１の発明は、前記利用者装置のコンピュータを、前記属性認可書の発行の際に、秘密鍵及び公開鍵を生成する鍵生成手段、入力された内容に基づいて前記ｎ個の属性情報を生成し、当該ｎ個の属性情報及び前記鍵生成手段により生成された公開鍵を前記属性認可書発行機関装置に提示する属性情報生成手段、前記属性認可書発行機関装置から受けた属性認可書を検証する属性認可書検証手段、として機能させ、前記検証者装置による検証の際に、前記属性認可書の検証用データと、チャレンジに基づいて計算した属性証明並びに前記ｎ個以下の属性情報の検証用データとを同時に又は別々に前記検証者装置に送信する属性証明生成手段、として機能させるための属性証明プログラムである。

【００１４】ここで、前記属性証明生成手段は、セキュリティ性向上の観点から、前記チャレンジのハッシュ値を算出し、このハッシュ値に基づいて前記属性証明を算出してもよい。

【００１５】また、前記属性証明生成手段は、利用者（証明者）が自分でチャレンジを生成する属性署名（属性付き署名）に適用する場合の観点から、「前記同時に又は別々に」に代えて「同時に」とし、且つ前記チャレンジを生成する処理を含めてもよい。

【００１６】第２の発明は、前記属性認可書発行機関装置のコンピュータを、前記利用者装置から提示された各属性情報に関して正当か否かを審査する属性情報審査手段、前記属性情報審査手段による審査結果が正当である旨を示すとき、前記ｎ個の属性情報を埋め込んで属性認可書を発行し、当該属性認可書を利用者装置に送信する属性認可書発行手段、として機能させるための属性証明プログラムである。

【００１７】第３の発明は、前記検証者装置のコンピュータを、前記利用者装置から受けた前記属性認可書の検証用データに基づいて、前記属性認可書の正当性を検証する属性認可書検証手段、前記属性認可書検証手段による検証結果が正当性を示すとき、前記利用者装置から受けた属性証明及び前記ｎ個以下の属性情報に関し、各々正当性を検証する属性証明検証手段、として機能させるための属性証明プログラムである。

【００１８】ここで、第３の発明は、検証者が自分でチャレンジを生成する場合に適用する観点から、前記属性認可書検証手段による検証結果が正当性を示すとき、ｎ個以下の属性を指定する属性情報生成手段、前記属性情報生成手段により属性が指定されると、チャレンジを生成し、当該チャレンジ及び前記指定内容を前記利用者装置に送信するチャレンジ生成手段、として機能させるための属性証明プログラムであってもよい。

【００１９】なお、第３の発明は、さらに、前記属性証明検証手段による検証結果が正当性を示すとき、前記開示されたｎ個以下の属性情報の内容に基づいて、所定の対象システムの実行を許可する対象実行許可手段、として機能させるための属性証明プログラムとしてもよい。

【００２０】（作用）従って、本発明は以上のような手段を講じたことにより、ｎ個の属性情報の埋め込まれた属性認可書を利用し、開示要求されるｎ個以下の属性情報のみを検証者に開示し、開示要求されない属性情報を隠蔽できる。

【００２１】このように、各種証明／署名の際に、属性情報を選択的に開示する属性証明システムを構築できるので、各種システムに応用でき、情報化社会の発展に寄与することができる。

【００２２】

【発明の実施の形態】以下、本発明の各実施形態について図面を参照して説明する。なお、各実施形態で使用される各種パラメータと記号は以下の通りである。

ｐ，ｑ：十分に大きな素数で$p=2q+1$の関係式を満たす。

ｇ：乗法群Z_p^*での位数がｑとなるような生成器。（ｇは、システム共通の値（第４を除く第１～第６実施形態）としてもよく、利用者装置Ａが生成する値（第４～第６実施形態）としてもよい）

P_A：利用者装置Ａの公開鍵。

S_A：利用者装置Ａの秘密鍵。

Λ_0：属性認可書発行時に提示された属性群$\{a_1, a_2, \cdots, a_n\}$。

a_i：Λ_0のｉ番目$(1 \leq i \leq n)$の属性情報（attribute）

ｎ：属性情報の総数

r_i：ｉ番目$(1 \leq i \leq n)$の乱数。

b_i：a_iのブラインド値（blinded attribute）

c_i：b_iのコミット値（committed blinded attribute）

ｈ：無衝突一方向性ハッシュ関数。

$Sig_{AcA}[D]$：データＤに対する属性認可書発行機関の署名。

$Veri_{AcA}[D]$：データＤに対する属性認可書発行機関の署名検証。

ｕ：属性証明時に利用者（証明者）装置Ａが生成する乱数（$\in_R Zq^*$）

ｖ：属性証明時に利用者（証明者）装置Ａが計算するｕのコミット値（$v=g^u \pmod p$）

Λ：属性証明時に開示要求のあった属性群。

ｍ：属性証明時に検証者装置Ｖが生成するチャレンジ（$\in Zq^*$）あるいは利用者装置Ａが生成する（このチャレンジの）ハッシュ値

ｆ(ｍ)：ｍを用いたΛの属性証明

ｘ||ｙ：ビット列ｘとビット列ｙとの結合。

【００２３】（第１の実施形態）図１は本発明の第１の実施形態に係る属性証明システムの構成を示す模式図である。この属性証明システムは、利用者装置Ａ、属性認可書発行機関装置ＡＣＡ及び検証者装置Ｖを備えており、各装置Ａ，ＡＣＡ，Ｖは、それぞれハードウェア、ソフトウェア又はそれらの組合せにより構成可能となっている。なお、ソフトウェアにより構成される場合、各装置Ａ，ＡＣＡ，Ｖの機能を実現するためのプログラムが各装置Ａ，ＡＣＡ，Ｖのコンピュータに予めインストールされている。

【００２４】利用者装置Ａは、鍵生成部１１、属性情報生成部１２、属性認可書検証部１３、属性情報管理部１４及び属性証明生成部１５を備えている。

【００２５】鍵生成部１１は、属性認可書$Cert_A$の発行前に、秘密鍵S_A及び公開鍵P_Aを生成し、属性認可書$Cert_A$の発行時に、これら秘密鍵S_A及び公開鍵P_Aを属性情報生成部１２に送出する機能をもっている。

【００２６】属性情報生成部１２は、鍵生成部１１から受けた秘密鍵S_Aを属性認可書検証部１３に設定する機能と、利用者の入力操作により、承認して欲しい属性情報$\{a_1,a_2,\cdots,a_n\}$を生成して属性情報管理部１４に設定する機能と、公開鍵P_Aと承認して欲しい属性情報からなる属性群$\Lambda_0=\{a_1,a_2,\cdots,a_n\}$とを属性認可書発行機関ＡＣＡに提示する機能とをもっている。なお、属性情報は、何らかの部分情報であればよく、その内容は任意である。

【００２７】属性認可書検証部１３は、属性認可書発行機関ＡＣＡから受けた属性認可書$Cert_A$及びｎ個の乱数（$r_1,\cdots,r_n$）に基づいて、属性情報管理部１４を参照しながら所定の検証処理（後述するＳＴ９）を行なう機能と、検証処理の終了後、属性認可書$Cert_A$及びｎ個の乱数（$r_1,\cdots,r_n$）を属性情報管理部１４に保存する機能とをもっている。

【００２８】なお、属性認可書$Cert_A$は、属性認可書発行機関装置ＡＣＡによるデジタル署名$Sig_{ACA}[h(P_A||n||c_1||\cdots||c_n)]$である。

【００２９】属性情報管理部１４は、利用者装置Ａ内の各情報を読出／書込可能に保持・管理するものであり、具体的には、公開鍵P_A、秘密鍵S_A、各属性a_1～a_n、各乱数r_1～r_n、各コミット値c_1～c_n及び属性認可書

$Cert_A$が管理可能となっている。なお、秘密鍵S_Aは、他の耐タンパー性メモリ（図示せず）で管理してもよい。

【００３０】属性証明生成部１５は、属性証明の際に、乱数ｕ及びそのコミット値ｖを生成する機能と、属性情報管理部１４を参照して検証用データ（$v,Cert_A,n,P_A,c_1,\cdots,c_n$）を検証者装置Ｖに送信する機能と、検証者装置Ｖからチャレンジｍ及び属性群Λを受けると、要求された属性の開示を容認する場合、属性証明ｆ(ｍ)を計算する機能と、この属性証明ｆ(ｍ)及びデータ(j,a_j,r_j)を検証者装置Ｖに送信する機能とをもっている。

【００３１】また、利用者装置Ａの実現形態としては、任意の形態が適用可能である。例えば、パーソナルコンピュータの如き設置型や可般型、又は携帯電話や電子手帳の如き携帯型、あるいはそれらの組合せ（例、設置型の装置と、携帯型のＩＣカードとの組合せ等）のいずれでもよく、その通信方式も有線又は無線のいずれでもよい。

【００３２】属性認可書発行機関装置ＡＣＡは、属性情報審査部２１及び属性認可書発行部２２を備えている。

【００３３】属性情報審査部２１は、利用者装置Ａから提示された属性群Λ_0内の各属性a_iを利用者の情報として正当か否かを審査する機能と、審査結果を属性認可書発行部２２に送出する機能とをもっている。

【００３４】属性認可書発行部２２は、属性情報審査部２１から受けた審査結果が正当である旨を示すとき、所定の属性認可書発行処理（後述するＳＴ５～ＳＴ８）を実行する機能と、属性認可書発行処理の終了後、属性認可書$Cert_A$、ｎ個の乱数（$r_1,\cdots,r_n$）を利用者装置Ａに送信する機能とをもっている。

【００３５】検証者装置Ｖは、属性認可書検証部３１、属性情報要求部３２、チャレンジ生成部３３及び属性証明検証部３４を備えている。

【００３６】属性認可書検証部３１は、利用者装置Ａから受けた検証用データ（$v,Cert_A,n,P_A,c_1,\cdots,c_n$）に基づいて、属性認可書$Cert_A$の正当性を検証する機能と、検証結果を属性情報要求部３２に送出する機能とをもっている。

【００３７】属性情報要求部３２は、属性認可書検証部３１から受けた検証結果が正当を示すとき、開示して欲しい属性（要求属性）からなる属性群Λをチャレンジ生成部３３に送出する機能をもっている。

【００３８】チャレンジ生成部３３は、属性情報要求部３２から属性群Λを受けると、チャレンジｍを生成する機能と、このチャレンジｍ及び属性群Λを属性証明検証部３４及び利用者装置Ａに送信する機能とをもっている。

【００３９】属性証明検証部３４は、利用者装置Ａから受けた属性証明ｆ(ｍ)の正当性を検証する機能と、この

検証結果が正当を示すとき、開示された属性a_iの正当性を検証する機能とをもっている。

【００４０】次に、以上のように構成された属性証明システムの動作を図２及び図３のフローチャートを用いて、初期手続時の属性認可書発行、及び通常使用時の属性証明の順に説明する。

【００４１】（属性認可書発行）図２に示すように、利用者装置Ａにおいては、鍵生成部１１が秘密鍵$S_A \in_R Z_q$を生成し（ＳＴ１）、公開鍵$P_A = g^{S_A} \pmod p$を計算すると（ＳＴ２）、これら秘密鍵S_A及び公開鍵P_Aを属性情報生成部１２に送出する。

【００４２】属性情報生成部１２は、秘密鍵S_Aを属性認可書検証部１３に設定し、承認して欲しい属性情報を生成して（ＳＴ３）属性情報管理部１４に設定する一方、公開鍵P_Aと、承認して欲しい属性情報からなる属性群Λ_0を属性認可書発行機関ＡＣＡに提示する。属性認可書発行機関ＡＣＡにおいては、属性情報審査部２１が、提示された各属性a_iを利用者の情報として正当か否かを審査し（ＳＴ４）、審査結果を属性認可書発行部２２に送出する。

【００４３】属性認可書発行部２２は、審査結果が正当である旨を示すとき、以下の属性認可書発行処理（ＳＴ５～ＳＴ８）を実行する。

【００４４】始めに、ｎ個の乱数$r_i \in_R Z_q^*$を生成する（ＳＴ５）。

【００４５】続いて、乱数r_iと属性a_iとを結合（連接）してハッシュ関数により、ｎ個のブラインド値$b_i = h(a_i||r_i)$を計算する（ＳＴ６）。

【００４６】次に、生成器ｇに対し、各ブラインド値b_iを用いてｎ個のコミット値$c_i = g^{b_i} \pmod p$を計算する（ＳＴ７）。

【００４７】最後に、公開鍵P_A，属性a_iの総数ｎ及び各コミット値ｃ1～ｃnを結合し、それらにハッシュ関数を介して得たハッシュ値に対し、自己の秘密鍵で署名を施すことにより、属性認可書$Cert_A$を発行する（ＳＴ８）。

【００４８】

$Cert_A = Sig_{ACA}[h(P_A||n||c_1||\cdots||c_n)]$

このような属性認可書発行処理の終了後、属性認可書発行機関ＡＣＡは、属性認可書$Cert_A$、ｎ個の乱数（r_1，…，r_n）を利用者装置Ａに送信する。

【００４９】一方、利用者装置Ａでは、属性認可書検証部１３が以下の検証処理を行う（ＳＴ９）。

【００５０】始めに、属性情報管理部１４からｎ個の属性a_1～a_nを得ると、これら各属性a_iと各乱数r_iとを結合してハッシュ関数により、ｎ個のブラインド値$b_i = h(a_i||r_i)$を計算する。

【００５１】次に、生成器ｇに対し、各ブラインド値b_iを用いて、$c_i = g^{b_i} \pmod p$を計算する。

【００５２】最後に、公開鍵P_A，属性a_iの総数ｎ及び各コミット値c_1～c_nを結合し、それらにハッシュ関数を介して得たハッシュ値と、属性認可書$Cert_A$を属性認可書発行機関ＡＣＡの公開鍵で復号した復号結果とを比較することにより、属性認可書$Cert_A$の署名を検証する。

【００５３】$Veri_{ACA}[h(P_A||n||c_1||\cdots||c_n), Cert_A] = valid$（正当）？

このような検証処理の終了後、検証結果が正当であれば、利用者装置Ａは、属性認可書$Cert_A$、各乱数r_1～r_n及び各コミット値c_1～c_nを属性情報管理部１４に保存する。

【００５４】（属性証明）図３に示すように、利用者装置Ａでは、属性証明生成部１５が、乱数$u \in_R Z_q^*$を生成し、そのコミット値$v = g^u \pmod p$を計算する（ＳＴ１１）。

【００５５】しかる後、属性証明生成部１５は、属性情報管理部１４を参照して、乱数ｕのコミット値ｖ、属性認可書$Cert_A$、属性a_1～a_nの総数ｎ、公開鍵P_A、属性a_1～a_nのコミット値$c_1,\cdots,c_n$からなる検証用データ$(v, Cert_A, n, P_A, c_1, \cdots, c_n)$を検証者装置Ｖに送信する。

【００５６】検証者装置Ｖは、属性認可書$Cert_A$の検証用データ$(v, Cert_A, n, P_A, c_1, \cdots, c_n)$を受けると、属性認可書検証部３１により、属性認可書$Cert_A$の正当性を検証する（ＳＴ１２）。

【００５７】$Veri_{ACA}[h(P_A||n||c_1||\cdots||c_n), Cert_A] = valid?$

これにより、検証者装置Ａは、属性認可書$Cert_A$内の全ての属性情報a_1～a_nが認可された正当な情報である旨を検証する。正当性の検証処理の終了後、属性認可書検証部３１は、検証結果を属性情報要求部３２に送出する。

【００５８】属性情報要求部３２は、検証結果が正当であれば、開示して欲しい属性（要求属性）からなる属性群Λをチャレンジ生成部３３に送出する。

【００５９】チャレンジ生成部３３は、チャレンジ$m \in_R Z_q^*$を生成し（ＳＴ１３）、チャレンジｍと、開示して欲しい属性からなる属性群Λとを自己の属性証明検証部３４及び利用者装置Ａに送信する。

【００６０】利用者装置Ａでは、チャレンジｍ及び属性群Λを受けると、属性証明生成部１５が、開示要求された属性に対し、開示を容認する場合、最大でｎ＋１次の多項式からなる属性証明ｆ(m)を計算する（ＳＴ１４）。

$f(m) = vS_A + um + b_1 m^2 + \cdots + b_n m^{n+1} \pmod q$

すなわち、属性証明ｆ(m)は、開示要求された属性の総数がｉ個の場合、次式のようにｉ＋１次となる。

$f(m) = vS_A + um + b_1 m^2 + \cdots + b_i m^{i+1} \pmod q$

なお、同式中の“b_1～b_i”の記載は、１番目～ｉ番目の値に限定される趣旨とは異なり、開示要求に対応したｉ個の“b_i”が用いられる趣旨であることは言うまでもない。これは後述するｆ(m)の検証式中の“c_i”でも同様である。また、変形例として、開示、非開示に関わらず、ｎ個全ての属性（b_1～b_n）で属性証明ｆ(m)を生成する構成としてもよい。

【００６１】いずれにしても、その後、属性証明生成部１５は、属性証明ｆ(m)と、開示要求のあった属性群Λに該当する属性番号ｊ、属性a_i及び乱数r_iからなる開示要求された属性情報の検証用データ(j, a_i, r_i)とを検証者装置Ｖに送信する（ｊ∈Λ）。

【００６２】検証者装置Ｖでは、属性証明検証部３４が、この属性証明ｆ(m)の正当性を次の第１検証式により検証する（ＳＴ１５）。

【数１】

$$g^{f(m)} \equiv P_A^v v^m \prod_{i=1}^{i} c_i^{m^{i+1}} \pmod{p}$$

【００６３】これにより、検証者装置Ｖは、属性認可書$Cert_A$内の全ての属性情報a_1～a_nのうち、開示要求されたｉ個の属性情報a_1～a_iの全てが認可された正当な情報であることを検証することができる。また、検証結果が正当を示すとき、属性証明検証部３４は、開示要求した属性ｊ∈Λについて、ステップＳＴ１２で受けたコミット値c_iを使い、開示された属性a_iの正当性を次の第２検証式のように個別に検証する（ＳＴ１６）。

【数２】

$$c_j \equiv g^{h(a_j \| r_j)} \pmod{p}$$

【００６４】これにより、検証者装置Ｖは、属性認可書$Cert_A$内のｎ個の属性a_1～a_nのうち、開示された属性a_iのみを個別に検証することができる。

【００６５】上述したように本実施形態によれば、ｎ個の属性情報a_1～a_nの埋め込まれた属性認可書$Cert_A$を利用し、開示要求されたｎ個以下の属性情報a_iのみを検証者装置Ｖに開示し、開示要求されない属性情報を隠蔽できる。

【００６６】このように、各種証明／署名の際に、属性情報a_iを選択的に開示する属性証明システムを構築できるので、各種システムに応用でき、情報化社会の発展に寄与することができる。

【００６７】すなわち、利用者装置Ａは、ステップＳＴ１２により、属性認可書$Cert_A$内の全ての属性情報a_1～a_nが認可された正当な情報であることを検証者装置Ｖに証明することができる。

【００６８】また、利用者装置Ａは、ステップＳＴ１５により、属性認可書$Cert_A$内の全ての属性情報a_1～a_nのうち、開示要求されたｉ個の属性情報a_1～a_iの全てが認可された正当な情報であることを検証者装置Ｖに証明することができる。

【００６９】さらに、利用者装置Ａは、ステップＳＴ１６により、各属性a_iを個別に証明できるので、必要最小限の属性a_iしか開示しなくとも済む。このため、開示要求されなかった属性情報を検証者から隠蔽・保護することができる。例えば、属性情報がプライバシーに関する内容である場合、開示要求されなかった属性情報に関するプライバシーを保護することができる。

【００７０】（第２の実施形態）次に、本発明の第２の実施形態に係る属性証明システムについて述べるが、第１の実施形態と同一部分についてはその詳しい説明を省略し、ここでは異なる部分について主に述べる。なお、以下の各実施形態についても同様にして重複した説明を省略する。すなわち、本実施形態は、第１の実施形態の変形例であり、セキュリティの向上を図るものであって、具体的には、属性証明ｆ(m)の生成過程において、属性証明に使用される値ｍを、チャレンジＭのハッシュ値ｍ＝ｈ(M)に変更した構成となっている。

【００７１】従って、本実施形態は、以下に述べる属性証明時のチャレンジに関する動作以外は第１の実施形態と同様の作用効果を有する。すなわち、本実施形態の属性証明時においては、検証者装置Ｖのチャレンジ生成部３３が、チャレンジｍではなく、チャレンジ$M \in_R Z_q^*$を生成して前述同様に（開示要求する属性群Λと共に）利用者装置Ａに送信する。

【００７２】利用者装置Ａの属性証明生成部１５は、チャレンジＭのハッシュ値ｍ＝ｈ(M)を計算し、このハッシュ値ｍに対する属性証明ｆ(m)を前述同様に計算し、前述同様に（検証用データ（ｊ,a_i,r_i）と共に）検証者装置Ｖに送信する。

【００７３】また、検証者装置Ｖの属性証明検証部３４は、利用者装置Ａから属性証明ｆ(m)を受けると、チャレンジＭのハッシュ値ｍ＝ｈ(M)を計算した後、このハッシュ値ｍを用いて前述同様に属性証明ｆ(m)の正当性を検証する。以下、第１の実施形態と同様に動作する。

【００７４】上述したように本実施形態によれば、第１の実施形態の効果に加え、チャレンジＭのハッシュ値ｍ＝ｈ(M)に対して属性証明ｆ(m)を行なうことから、セキュリティ性を向上させることができる。

【００７５】（第３の実施形態）図４は本発明の第３の実施形態に係る属性証明システムの構成を示す模式図である。本実施形態は、第１及び第２の実施形態の変形例であり、第１及び第２の実施形態と異なる点は、チャレンジＭが利用者（証明者）装置Ａにより生成される点である。すなわち、本実施形態は、属性証明の一種として、自己の文書（チャレンジ）Ｍに対する属性署名（属性付き署名）を実現するものである。

【００７６】具体的には利用者装置Ａの属性証明生成部１５が、前述した機能に加え、文書Ｍとしてのチャレンジを生成し、このチャレンジＭのハッシュ値ｍ＝ｈ

(M)を算出し、このハッシュ値mの属性証明（文書Mに対する署名）f(m)を算出し、且つ（検証者装置Vからの開示要求無しに）開示する属性群Λを用意し、これらチャレンジM、属性証明f(m)、属性群Λの検証用データを検証者装置Vに送信可能な構成となっている。

【００７７】ここで、文書Mとしては、属性署名の対象となる電子化文書であれば任意の文書が使用可能であり、その種の電子化文書の典型的な例としては、アンケート調査の回答文書などがある。開示する属性としては、前述同様に必要最小限の属性であり、例えば「性別（例、男性）」、「年齢（例、２６歳）」、「職業（例、会社員）」等がある。なお、開示する属性は、ここでは利用者装置Aに用意される場合を述べたが、第１及び第２の実施形態と同じく、検証者装置Vから要求されてもよい。

【００７８】一方、検証者装置Vでは、属性情報要求部３２及びチャレンジ生成部３３が省略された構成となる。これに伴い、属性認可書検証部３１は、前述した機能において、属性認可書$Cert_A$の検証結果の送出先が属性証明検証部３４'になっている。

【００７９】属性証明検証部３４'は、前述した機能に加え、利用者装置Aから受けたチャレンジMを用いてそのハッシュ値m＝h(M)を計算する機能と、得られたハッシュ値mを用いて前述同様に属性証明f(m)の正当性を検証する機能をもっている。

【００８０】以上のような構成により、属性証明時に、利用者装置Aの属性証明生成部１５は、前述した機能に加え、チャレンジMを生成し、そのハッシュ値m＝h(M)を計算し、ハッシュ値mを用いた属性証明f(m)を計算する。また、開示する属性群Λの検証用情報を用意する。

【００８１】しかる後、利用者装置Aの属性証明生成部１５は、属性認可書$Cert_A$の検証用データ（v,$Cert_A$,n,P_A,c_1,…,c_n）、チャレンジM、属性証明f(m)、開示する属性情報の検証用データ(j,a_j,r_j)を検証者装置Vに送信する。

【００８２】検証者装置Vでは、これらを受けると、属性認可書検証部３１が、前述した通り、属性認可書$Cert_A$の検証用データ（v,$Cert_A$,n,P_A,c_1,…,c_n）に基づいて属性認可書$Cert_A$を検証し、検証結果を属性証明検証部３４'に送出する。

【００８３】属性証明検証部３４'は、検証結果が属性認可書$Cert_A$の正当性を示すとき、利用者装置Aから受けたチャレンジMを用いてそのハッシュ値m＝h(M)を計算し、このハッシュ値mを用いて前述同様に属性証明f(m)の正当性を検証する。以下、第１の実施形態と同様に動作する。

【００８４】上述したように本実施形態によれば、第１及び第２の実施形態の効果に加え、さらに、利用者（証明者）が自らチャレンジMを生成して属性署名（属性付き署名）を行なうことができる。この属性署名は、例えばアンケート調査の回答文書Mとしてのチャレンジなどのハッシュ値m＝h(M)に対して実施できる。

【００８５】なお、本実施形態の変形例として、開示する属性が、第１及び第２の実施形態と同じく、検証者装置Vから要求されてもよい。この変形例の場合、属性証明時に、利用者装置Aの属性証明生成部１５は、属性証明時に、第１の実施形態と同じく、属性認可書$Cert_A$の検証用データ（v,$Cert_A$,n,P_A,c_1,…,c_n）を検証者装置Vに送信し、検証者装置Vの属性認可書検証部３１は、前述した通り、属性認可書$Cert_A$の検証結果を属性証明検証部３４'に送出する。属性証明検証部３４'は、検証結果が属性認可書$Cert_A$の正当性を示すとき、開示して欲しい属性からなる属性群Λを利用者装置Aに送信する。利用者装置Aでは、属性群Λを受けると、属性証明生成部１５が、チャレンジMを生成し、そのハッシュ値m＝h(M)を計算し、ハッシュ値mを用いた属性証明f(m)を計算する。また、開示する属性群Λの検証用情報を用意する。といった動作となる。このような変形例としても本発明を同様に実施して同様の効果を得ることができる。

【００８６】（第４の実施形態）次に、本発明の第４の実施形態に係る属性証明システムについて説明する。

【００８７】本実施形態は、第１～第３の実施形態の変形例であり、生成器gを利用者装置Aが生成する値とし、属性認可書発行時に、生成器gを利用者装置Aから属性認可書発行機関装置ＡＣＡに提示する方式となっている。

【００８８】これに伴い、利用者装置A、属性認可書発行機関装置ＡＣＡ及び検証者装置Vの構成が以下のように変更される。利用者装置Aにおいては、鍵生成部１１が、前述した機能に加え、生成器gを生成する機能を有する。

【００８９】属性情報生成部１２は、前述した機能に加え、属性認可書発行機関装置ＡＣＡに対し、前述した情報（P_A, Λ_0）と、生成器gとを提示する機能を有する。

【００９０】属性証明生成部１５は、前述した機能に加え、生成器gを含めて属性情報の検証用データ（g,v,$Cert_A$,n,P_A,c_1,…,c_n）を検証者装置Vに送信する機能をもっている。

【００９１】一方、属性認可書発行機関装置ＡＣＡにおいては、属性認可書発行部２２が、前述した機能に加え、属性認可書発行時に、下記のように、生成器gを含めた内容の属性認可書$Cert_A$を発行する機能をもっている。

【００９２】$Cert_A = Sig_{ACA}[h(g||P_A||n||c_1||\cdots||c_n)]$ また一方、検証者装置Vにおいては、属性認可書検証部３１が、前述した機能に加え、下記のように、生成器gを含めた内容の属性認可書$Cert_A$を検証す

る機能をもっている。

【００９３】$Veri_{AcA}[h(g||P_A||n||c_1||\cdots||c_n), Cert_A]$＝valid?以上のような構成としても、第１～第３の実施形態と同様の効果を得ることができる。

【００９４】（第５の実施形態）図５は本発明の第５の実施形態に係る検証者装置の構成を示す模式図である。本実施形態は、第１～第５の実施形態の変形例であり、具体的には検証者装置Ｖが、属性証明検証部３４による検証結果に応じて後段の対象システムを利用可能とする対象実行許可部３５を備えている。

【００９５】ここで、対象実行許可部３５は、属性証明検証部３５により検証された属性と所定の判定基準とに基づいて、後段の対象システムの実行可否を判定し、実行可の時に実行を許可する機能をもっている。実行可否の判定基準は、任意であり、例えば属性が「男性」で判定基準が「男性」というように完全一致の場合や、属性が「２６歳」で判定基準が「２０歳以上」というように範囲指定の場合などが使用可能であり、その他、判定基準を検索条件と考えれば周知の検索技術などが適用可能である。

【００９６】対象システムの個数及び内容は任意であるが、例えば、「２０歳以上」「独身」「男性」の属性が証明された利用者にのみ閲覧させるホームページ等としてもよい。または、「本人」の属性が証明された利用者にのみ証明書を発行するシステム等がある。あるいは、任意の属性と、「属性認可書$Cert_A$の発行（要求）日」の属性とが証明され、且つ「属性認可書$Cert_A$の発行（要求）日」が有効期限内である利用者のみ実行可能なシステム等がある。

【００９７】すなわち、対象実行許可部３５は、任意の属性、当該属性に基づく実行可否の判定基準及び各種の対象システムに適用でき、それら実行可否の判定基準や対象システムの内容には限定がない。

【００９８】以上のような構成により、第１～第４の実施形態の効果に加え、後段の対象システムを不正な利用者による利用から保護することができる。

【００９９】なお、本実施形態は、対象実行許可部３５が実行可否を判定する場合を説明したが、実行可否に加え、対象実行許可部３５が、検証された属性に基づいて、利用可能な範囲をも設定する機能を有してもよい。

【０１００】例えば、機密事項ＤＢ及び周知資料ＤＢを有する社内システムの場合、「正社員」の属性をもつ利用者は、社内システム自体と周知資料ＤＢとを利用可能であるが、必ずしも機密事項ＤＢを利用できず、機密事項ＤＢを利用するには更に「機密事項ＤＢの担当部門」及び／又は「部長」以上の属性を必要とする等のように、検証された属性に基づいて、対象システムの実行可能な範囲を定めてもよい。

【０１０１】あるいは、対象システムが複数の実行パラメータをもつ場合（例、シミュレーションシステム、ロールプレイングゲームシステム、占いゲームシステム等）、システム全体を実行可能であるが、対象実行許可部３５が、検証された属性に基づいて、実行パラメータを設定する機能を備えてもよい。

【０１０２】（第６の実施形態）次に、本発明の第６の実施形態に係る属性証明システムについて説明する。本実施形態は、第１～第５の各実施形態の変形例であり、概略的には、第１～第５の各実施形態における離散対数問題を、有限群Ｅ（$GF(p)$）上の楕円離散対数問題（ＥＤＬＰ）に書換えた構成となっている。

【０１０３】ここで、有限群Ｅ（$GF(p)$）は、有限体$GF(p)$上の楕円曲線を意味しており、$a, b \in GF(p)$を$4a^3+27b^2 \neq 0$なる元とするとき、

$\{(x, y) \in GF(p)^2 \mid y^2 = x^3 + ax + b\} \cup O$

と表現される。但し、Ｏ：仮想的な無限遠点。

【０１０４】すなわち、本実施形態は、第１～第５の各実施形態を楕円曲線暗号に適用した変形例である。具体的には、第１の実施形態に明記され且つ第２～第５の各実施形態に引用される各式が以下のように書換えられる。なお、Ｇは楕円曲線上の点とする。

【０１０５】公開鍵$P_A = S_A \cdot G \pmod p$

（＝Ｇ＋…＋Ｇ：ＧをS_A回加算）

コミット値$C_i = b_i \cdot G \pmod p$

コミット値$V = u \cdot G \pmod p$

【数３】

$$\text{第１検証式 } f(m) \cdot G \equiv V P_A + mV + \sum_{i=1}^{i} m^{i+1} C_i \pmod p$$

第２検証式$C_i \equiv h(a_i||r_i) \cdot G \pmod p$

以上のような構成としても、第１～第５の各実施形態の効果を得ることができ、さらに楕円曲線暗号で実現したことにより、鍵長や署名データ長を低減させることができる。なお、上記実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【０１０６】また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【０１０７】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ

（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【０１０８】さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【０１０９】また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【０１１０】尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【０１１１】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０１１２】なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。例えば「属性情報」の語は、１個で独立して意味をもつ単位情報（例、単語、名称や小文書など、完結した情報）に限らず、全部又はしきい値個数以上が統合されると意味をもつ分散情報（例、秘密情報の一部）であってもよい。すなわち、「属性情報」の語は、任意の部分情報であればよく、社会通念上の「属性（その物の有する特徴・性質）」を示す内容ではなくても、本発明の範囲に包含される。

【０１１３】例えば、本発明を周知の段階的秘密交換プロトコルの適用対象（例、電子商取引など）に適用し、秘密情報（例、決済情報や契約文書）を所定サイズ毎に属性情報とした場合、社会通念上「決済情報や契約文書の一部」を示す内容であっても、本発明の「属性」に包含される。

【０１１４】但し、この場合、利用者装置と検証者装置の機能を併せもつ２台の利用・検証者装置が使用され、互いに選択的な属性情報の開示を繰り返し、最終的には全ての属性情報を開示し合うという構成になる。すなわち、属性情報の選択的な開示は、１回に限らず、複数回繰り返してもよい。また、利用者装置Ａと検証者装置Ｖとは、一方向で固定的な場合に限らず、双方向で交替的な場合も可能である。

【０１１５】一方、属性情報の定義に伴い、「属性認可書」の語は、各部分情報（各属性情報）の集合に対するデジタル署名であればよく、社会通念上の「属性を認可」したものでなくても本発明の範囲に包含される。前述の例では、社会通念上の「決済情報や契約文書」が本発明の「属性認可書」に包含される。

【０１１６】また、「利用者装置」及び「検証者装置」の語は、上述した機能を有するものであれば、社会通念上の「利用者」「検証者」には限定されない。例えば、本発明を「数字（属性情報）を揃えるスピードくじ」に適用する場合、スピードくじ（属性認可書）の販売者が「利用者装置」を用い、社会通念上の利用者が「検証者装置」を使うことになるが、このような場合も本発明の範囲に包含される。

【０１１７】また、各実施形態及び変形例は可能な限り適宜組み合わせて実施してもよく、その場合、組み合わされた効果が得られる。また、各実施形態及び変形例の組合せに限らず、各装置（利用者装置Ａ、属性認可書発行機関装置ＡＣＡ、検証者装置Ｖ）も、適用されるシステムに応じて適宜組合せて実施できる。

【０１１８】例えば、第１～第６の実施形態の場合、属性認可書発行機関装置ＡＣＡと検証者装置Ｖとを組合せてもよい。また、前述したスピードくじのシステムの場合等では、利用者装置Ａと属性認可書発行機関装置ＡＣＡとを組合せてもよい。さらに、前述した段階的秘密交換のシステムの場合等では、利用者装置Ａと検証者装置Ｖとを組合せてもよい。

【０１１９】さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成用件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【０１２０】その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【０１２１】

【発明の効果】以上説明したように本発明によれば、各種システムに応用でき、情報化社会の発展に寄与できる属性証明プログラム及び装置を提供できる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る属性証明システムの構成を示す模式図

【図２】同実施形態における属性認可書発行の動作を説明するためのフローチャート

【図３】同実施形態における属性証明の動作を説明するためのフローチャート

【図４】本発明の第３の実施形態に係る属性証明システムの構成を示す模式図

【図５】本発明の第５の実施形態に係る検証者装置の構成を示す模式図

【図６】本発明の骨子を説明するための模式図

【図７】本発明の骨子を従来と比較して説明するための模式図

【符号の説明】

Ａ…利用者装置

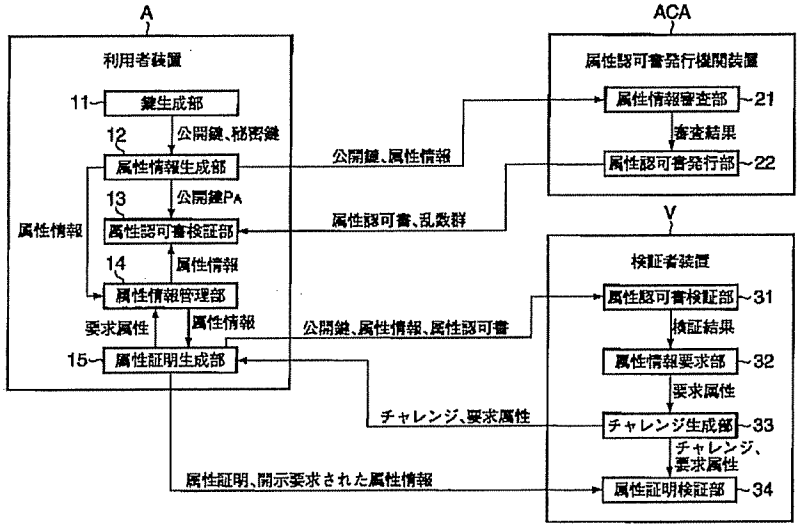
19

１１…鍵生成部
１２…属性情報生成部
１３…属性認可書検証部
１４…属性情報管理部
１５…属性証明生成部
ＡＣＡ…属性認可書発行機関装置
２１…属性情報審査部

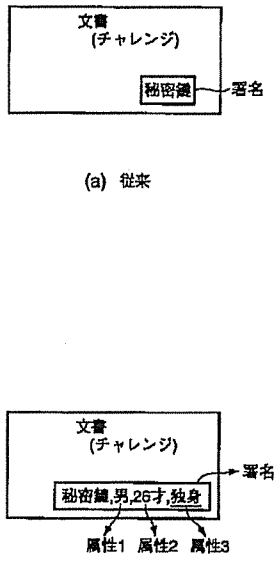
20

＊２２…属性認可書発行部
Ｖ…検証者装置
３１…属性認可書検証部
３２…属性情報要求部
３３…チャレンジ生成部
３４，３４’…属性証明検証部
＊

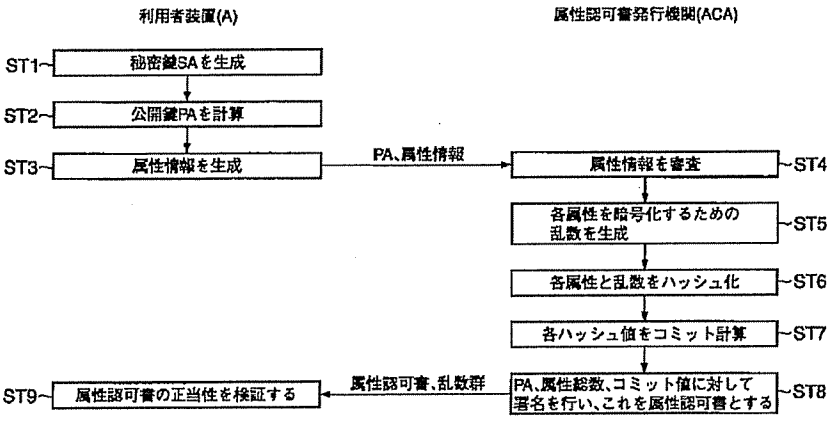
【図１】



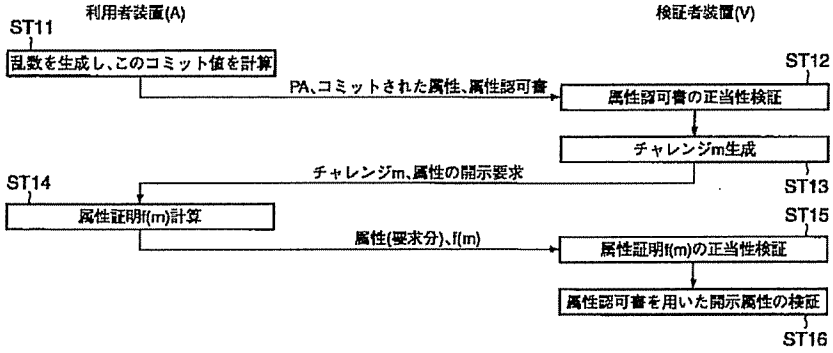
【図７】



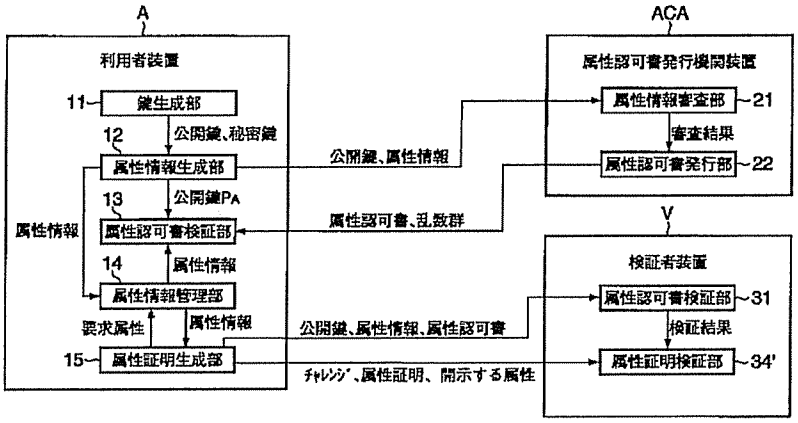
【図２】



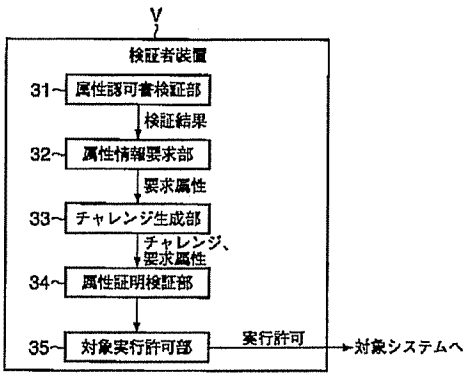
【図３】


利用者装置(A)
検証者装置(V)
ST11
乱数を生成し、このコミット値を計算
PA、コミットされた属性、属性認可書
ST12
属性認可書の正当性検証
チャレンジm生成
ST13
チャレンジm、属性の開示要求
ST14
属性証明f(m)計算
ST15
属性(要求分)、f(m)
属性証明f(m)の正当性検証
属性認可書を用いた開示属性の検証
ST16

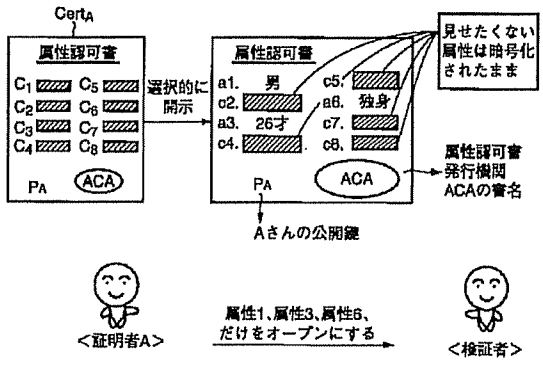
【図４】


A
利用者装置
11
鍵生成部
12
公開鍵、秘密鍵
属性情報生成部
公開鍵、属性情報
13
公開鍵PA
属性情報
属性認可書検証部
属性認可書、乱数群
14
属性情報
属性情報管理部
要求属性
属性情報
15
属性証明生成部
チャレンジ、属性証明、開示する属性
ACA
属性認可書発行機関装置
属性情報審査部
21
審査結果
属性認可書発行部
22
V
検証者装置
属性認可書検証部
31
検証結果
公開鍵、属性情報、属性認可書
属性証明検証部
34'

【図５】


V
検証者装置
31
属性認可書検証部
検証結果
32
属性情報要求部
要求属性
33
チャレンジ生成部
チャレンジ、
要求属性
34
属性証明検証部
35
対象実行許可部
実行許可
対象システムへ

【図６】


CertA
属性認可書
C1 C5
C2 C6
C3 C7
C4 C8
PA
ACA
選択的に
開示
属性認可書
a1. 男
c2.
a3. 26才
c4.
c5.
a6. 独身
c7.
c8.
PA
ACA
Aさんの公開鍵
見せたくない
属性は暗号化
されたまま
属性認可書
発行機関
ACAの署名
<証明者A>
属性1、属性3、属性6、
だけをオープンにする
<検証者>